Informal Meeting of the Justice and Home Affairs Ministers, Amsterdam 25-26 January 2016

Discussion Paper on tackling cybercrime

Meeting of Ministers of Justice, 26 January 2016

The criminal use of cyberspace

Cyberspace is borderless. Information flows freely between countries providing citizens and organisations almost unlimited access to information and digital services. Information is everywhere; the physical location of the servers on which it is stored is often not known and deemed irrelevant to users. Information can be stored, changed and deleted, and internet services can be used from anywhere in the world. Cyberspace has grown into an essential element of modern life.

The protection of cyberspace from incidents, malicious activities and misuse has become crucial for the functioning of our societies and economies. The borderless nature of cyberspace poses special challenges and opportunities for law enforcement and judicial authorities. Important information for law enforcement and judicial authorities, such as electronic evidence, can also be stored, changed and deleted in seconds. It can be stored in one country by criminals located in another country, and moved when they suspect law enforcement is catching up to them. The current procedures for mutual legal assistance (MLA) are complex, time consuming, and not adapted to the requirements of cyber investigations leaving law enforcement and juridical authorities far behind technically capable criminals. When criminals hide the location of their activities and identities with technical methods these MLA procedures become inadequate. In those cases it is not even known which country to request assistance from. Law enforcement agencies often rely on internet service providers to provide e-evidence. However, the laws for obtaining e-evidence are not identical in all countries. Internet service providers themselves, who are mostly willing to cooperate with law enforcement and judicial authorities if legally required, often have to cross borders to retrieve information, making it possible to violate laws in one country simply by complying in another.

Criminals know law enforcement and judicial authorities struggles to cope with these issues and they exploit these. They use technical means to hide their identity and move their criminal activity between countries, using the snail's pace of existing procedures to their advantage. They also often know which countries do not have the necessary legal framework, capability or legal assistance processes in place to fight them effectively. They can use these countries as safe havens for their criminal activities. By effectively evading the rule of law they enjoy an impunity that is unacceptable.

European action

The EU has recognized the challenge cyber criminality poses and has acted accordingly. Almost all Member States are party to the Budapest Convention on Cybercrime, providing a baseline for tackling cybercrime and for enhanced cooperation across borders. Europol and Eurojust have stepped up to the challenge of enhancing international cooperation both between Member States and with third countries. The European Cyber Crime Centre (EC3) has evolved into a vital hub for international cybercrime investigations. Several Joint Investigation Teams were successful and the efficiency of legal assistance procedures has increased. The implementation of the European Directive regarding the European Investigation Order Directive in criminal matters will further improve cooperation between member states also for cyber investigations.

Remaining challenges

Unfortunately, some challenges remain unaddressed. Criminals who are technically

nl EU 2016

capable or hide in countries with limited law enforcement capabilities against cybercrime are well able to evade prosecution. Cyberspace still gives criminals the opportunity to make large gains with little risk and technically advanced criminals can find a safe have in cyberspace. Two types of situations remain especially challenging:

1. Mutual legal assistance is not possible because the location of information or the origin of a cyber-attack is not known. Various effective ways to hide information about the location of information and activities have been developed and some hosting providers offer hosting in countries of choice, allowing criminals to choose countries with limited law enforcement capabilities. This is called “bullet proof hosting”. These hosters promise their clients not to log their activities and to inform them when law enforcement and judicial agencies are requesting their data. Criminals use these hosters to store stolen data, including credit card information, data for botnet herding or child abuse images in those countries. Dedicated communication servers are another example. Criminals can use their own enterprise server to direct their communications while applying strong encryption techniques. Eavesdropping is not effective because of the encryption, and data from the server cannot be obtained, because it is located in the criminal’s country of choice. There seems to be a lively trade in these kind of servers. TOR and I2P techniques are a third example. Although these techniques of course also allow for legal use most TOR and I2P traffic is of a criminal nature, in particular the trade in drugs and weapons and the spread of child abuse images. Identifying criminals, both buyers and sellers, is often not possible and many criminals are untouchable.

   In these situations mutual legal assistance is not possible, no matter how efficient procedures are. In these circumstances, stopping a cyber-attack or acquiring e-evidence could violate the sovereignty of another country. In most cases this is not allowed under international law. MLA can also be impossible for other reasons. For example, the countries involved could have only limited relations or be involved in diplomatic issues. Second, legal differences could limit the possibilities for assistance. Investigative powers can differ, or the dual criminality requirement might not be met. Third, the country could lack effective capabilities for handling cybercrime and mutual legal assistance requests. Fourth, criminals move their activities to other countries either regularly or when they suspect they are being investigated by law enforcement and judicial authorities, staying ahead of these agencies due to slow MLA procedures. These examples often involve countries outside the EU.

2. Conflicting regulations hamper cooperation with private parties. Internet service providers, especially those providing cloud computing services, often do not store information about clients and their activities in the countries where those clients are. Those private companies may even be established in one country while also providing their services in other countries. Suspects of criminal investigations can be located in one country while information about them is in another. It can be necessary for law enforcement and judicial authorities to request information physically stored in another country. For internet service providers, differences in regulations can become an obstacle for cooperation. Complying with a request for data in one country could imply breaking the law in the other.

   In situations as described in the above, the investigation and any further action taken against cybercrime comes to a halt. These challenges cannot be resolved by further improving cooperation. The European Agenda on Security[1] recognises that this state of affairs is unacceptable and prioritises “*reviewing the obstacles to criminal investigations on cybercrime, notably on issues of competent jurisdiction and rules on access to evidence and information*”.

Common interest: the security of cyberspace

The security of cyberspace is of common interest to law enforcement and judicial authorities, citizens, private organisations and other parts of government. Solutions for these challenges should therefore take into account interests of all these parties.

Law enforcement and judicial authorities are charged with upholding the rule of law within the appropriate legal framework, also in cyberspace. People and businesses should be protected against crime. A secure internet is vital to society. Law enforcement and judicial authorities should be given the ability to improve that security for social and economic activities and to counter crime. The legal framework should provide law enforcement and judicial authorities with the

1 Doc. 8293/15

powers necessary to perform their duties effectively. At the same time, the investigative powers they hold can intrude into private lives and business processes. Everyone should be confident that law enforcement and judicial authorities will only use their investigative powers under strict conditions, their use being lawful, necessary and proportionate and subject to proper procedural safeguards. Proper regulation and transparency about the use of investigative powers are essential for people and businesses to trust the law enforcement and judicial authorities and for their trust in cyberspace being safe and secure.

Private enterprises are often valuable partners in the fight against cybercrime. The private sector not only has the information necessary to solve individual cases because of their control of applications on the internet but also has valuable knowledge about cyberspace and the possibilities it provides for effective investigation. So as to ensure that the cooperation with private partners remains constructive, clear regulations and points of contact are required. Moreover, the issue of conflicting regulations should be addressed.

EU process

Following the adoption of the EU Agenda on Security, valuable contributions were made to the debate on jurisdiction in cyberspace during Luxembourg's EU presidency term. The current paper serves as a basis for an informal discussion at the ministerial level during their EU presidency term. Current practices in joint cybercrime operations are set to be evaluated through EMPACT. This is to be followed up on by an expert-level conference to build on the insights gained thus far. The results will thereafter be discussed by COSI and CATS, possibly leading to the development of a further programme of action.

In the light of the above, ministers are invited to discuss the following questions[2]*:*

1. Do you support the development of a common view on jurisdiction in cyberspace in addition to improving operational cooperation?
2. Which issues do you think could be addressed in that respect and what is your view on those issues?
3. Do we need alternative approaches (e.g. legal or other instruments) for situations when mutual legal assistance is not possible?
4. Which alternatives would you propose?
5. Conflicting national and international regulations regarding e-evidence hamper cooperation with private parties. Should we develop a common approach to tackle this issue?
6. Which elements should be part of such a common approach?

[2] As mentioned in the cover note, you are kindly invited to share (an outline of) your Minister's response with the Presidency in advance, which will support us in focusing the discussion in the meeting on those points which require the most attention.

nl EU 2016